

Oracle Critical Patch Updates: Insight and Understanding

Stephen Kost
Integrigy Corporation

Introduction

- **Stephen Kost**

- Chief Technology Officer of Integrigy Corporation
- 12 years experience with Oracle Applications as Applications DBA, architect, and application administrator
- Found more than 40 security bugs fixed in CPUs

- **Integrigy Corporation**

- Only firm that is dedicated to Oracle E-Business Suite Security
- Services – Oracle Applications Security Assessments
- Products – AppSentry and AppDefend

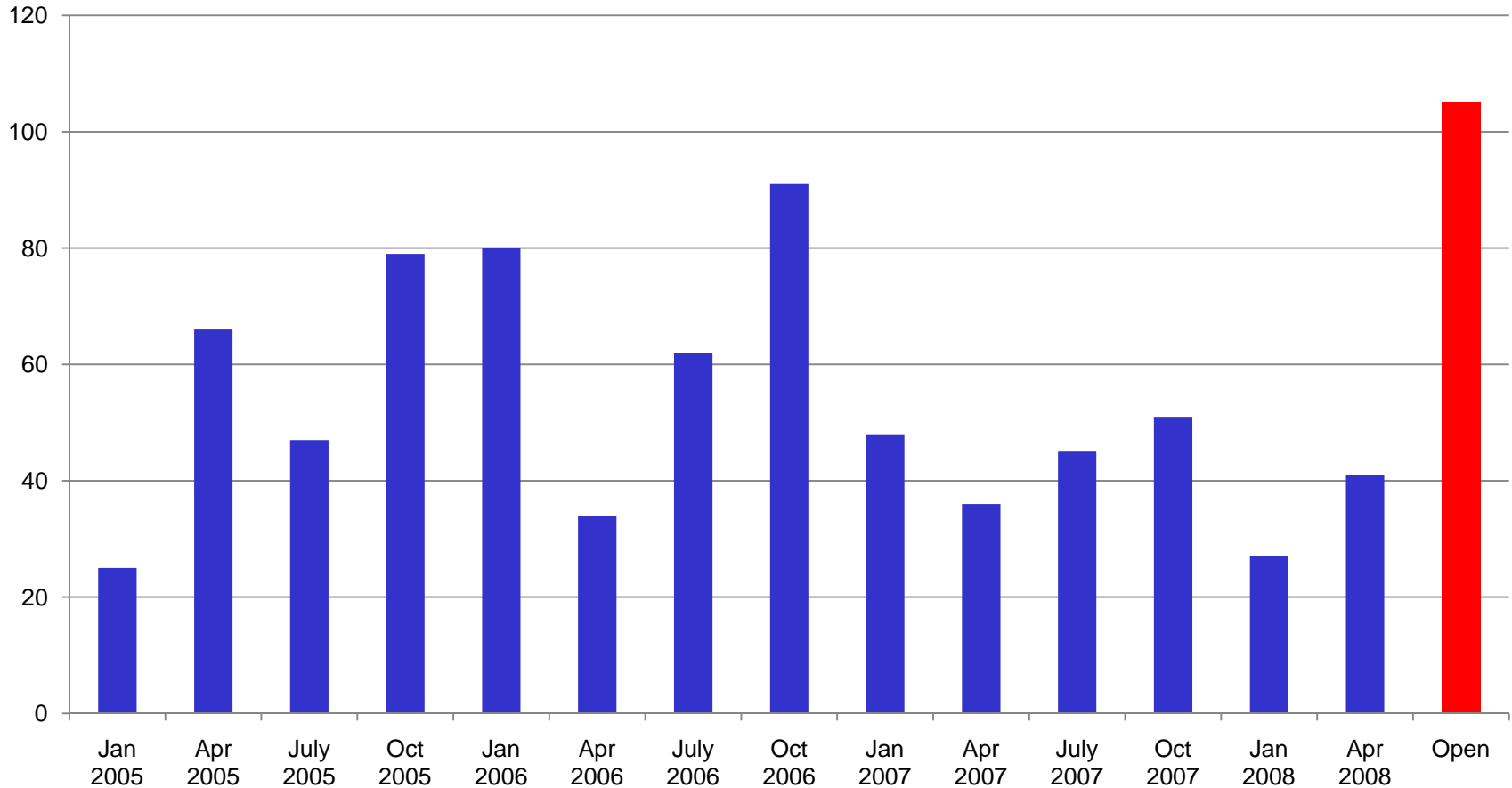
Agenda

- Background of Critical Patch Updates
- Vulnerabilities
- Certification vs. Certification
- Patches
- Patching Strategy
- Questions

Oracle Critical Patch Updates

- Fixes for security bugs in all Oracle products
 - Released quarterly on a fixed schedule
 - Tuesday closest to the 15th day of January, April, July and October
 - Next CPUs = April 15, 2008 (today) and July 15, 2008
- Fourteen CPUs released to date starting with Jan 2005
 - 732 security bugs fixed (average is 53 bugs per CPU)
 - 323 bugs in the Oracle Database
 - 164 bugs in the Oracle E-Business Suite 11i

Security Bugs per CPU (all products)



Security Bug Process

Bug reported

1. Customer or security researcher reports security bug to Oracle
2. Oracle researches bug and develops bug fix
 - Finder not allowed to test fix or even notified about fix
3. Oracle may include fix in new releases
 - No notification of security fixes to customers
4. Oracle includes fix in quarterly CPU
 - **From initial report to security patch release is 3 months to 3 years**

Elapsed time on average is 18 months

Bug fixed

Types of Oracle Security Bugs

- Buffer Overflow
- SQL Injection
- Cross-site Scripting (XSS)
- Parameter Tampering
- Permission Issues
- Information Disclosure

% of Bugs Exploitable with No Auth

4%

For the CPUs January 2007 through January 2008 (3 of 81 database bugs)

% of Bugs PUBLIC Exploitable

44%

For the CPUs January 2007 through January 2008 (36 of 81 database bugs)

% of Published Exploits PUBLIC Exploitable

89%

For the CPUs January 2007 through January 2008 (16 of 18 database bugs)

Who can exploit a PUBLIC bug?

APPLSYS/PUB/PUB

and anyone else with a database account

Database Vulnerabilities (Jan08/11i)

Supported Database Version ¹	PUBLIC (i.e., APPLSYSPUB)	Other Privileges (CREATE VIEW)	No Default Privileges
9.2.0.8	DB04 – SDO_CATALOG DB06 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM DB03 - DBMS_PRVTAQIP
10.1.0.5	DB04 – SDO_CATALOG DB06 – Oracle Spatial DB07 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM DB03 - DBMS_PRVTAQIP
10.2.0.2/ 10.2.0.3	DB04 – SDO_CATALOG DB07 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM

Oracle Applications 11i Baseline

- Critical Patch Updates require an Oracle Applications 11i minimum ATG_PF.H RUP level
 - Starting in July 2007, must be RUP(n) or RUP(n-1)
 - RUP(n) or RUP(n-1) for all versions 11.5.9 through 11.5.10.2
 - January 2008 requires RUP4, RUP5, or RUP6
 - **April 2008 requires RUP5 and RUP6 only**

Metalink Certification != CPU Certification

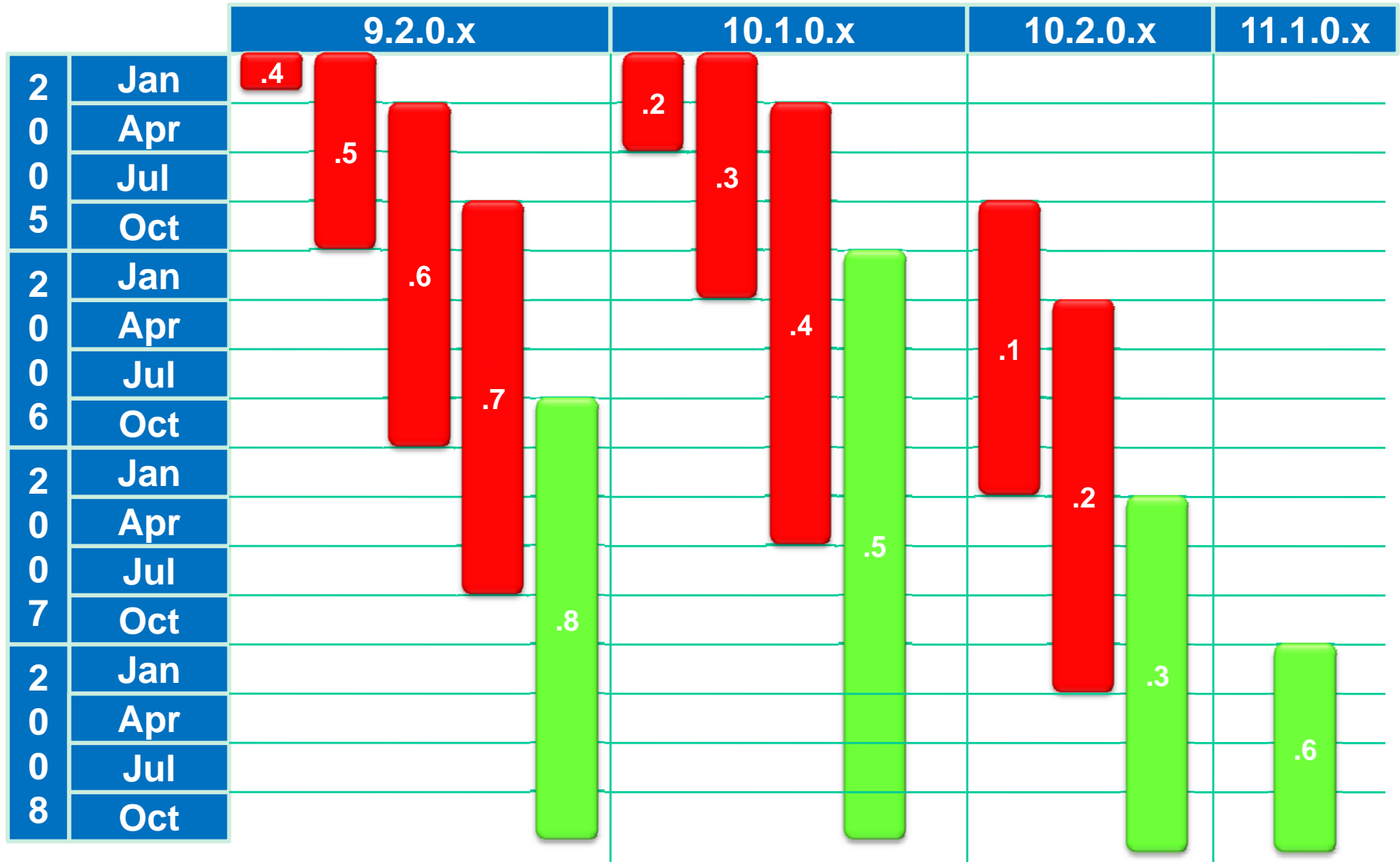
- Controlled by Oracle Software Error Correction Support Policy
- CPUs only certified with latest two patch sets released in the past 12 months

Apps Version	Database	App Server (Apache)	Developer	JInitiator (WinXP)	ATG_PF
11.5.10.2	9.2.0.4 9.2.0.5* 9.2.0.6 - 7 9.2.0.8 10.1.0.4 10.1.0.5 10.2.0.2 10.2.0.3	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.24 (P15)* 6.0.8.x (P16 - P17) 6.0.8.27 (P18)	1.1.8.19-25 1.1.8.27 1.3.1.18* 1.3.1.21 - 28 1.3.1.29	ATG_PF.H* ATG_PF.H RUP5 or ATG_PF.H RUP6

Chart is for
April 2008 CPU

Desupported
Certified, No CPU Support

Certified for CPU
* Fresh Install Version



CPU Certification Changes for April 2008

- Oracle Applications 11i
 - ATG_PF.H RUP5 or RUP6
 - No support for 11.5.8 (ended October 2008)
- Oracle Database
 - 10.2.0.2 = No support
- Oracle Application Server
 - No changes

CPU Certification Changes - Future

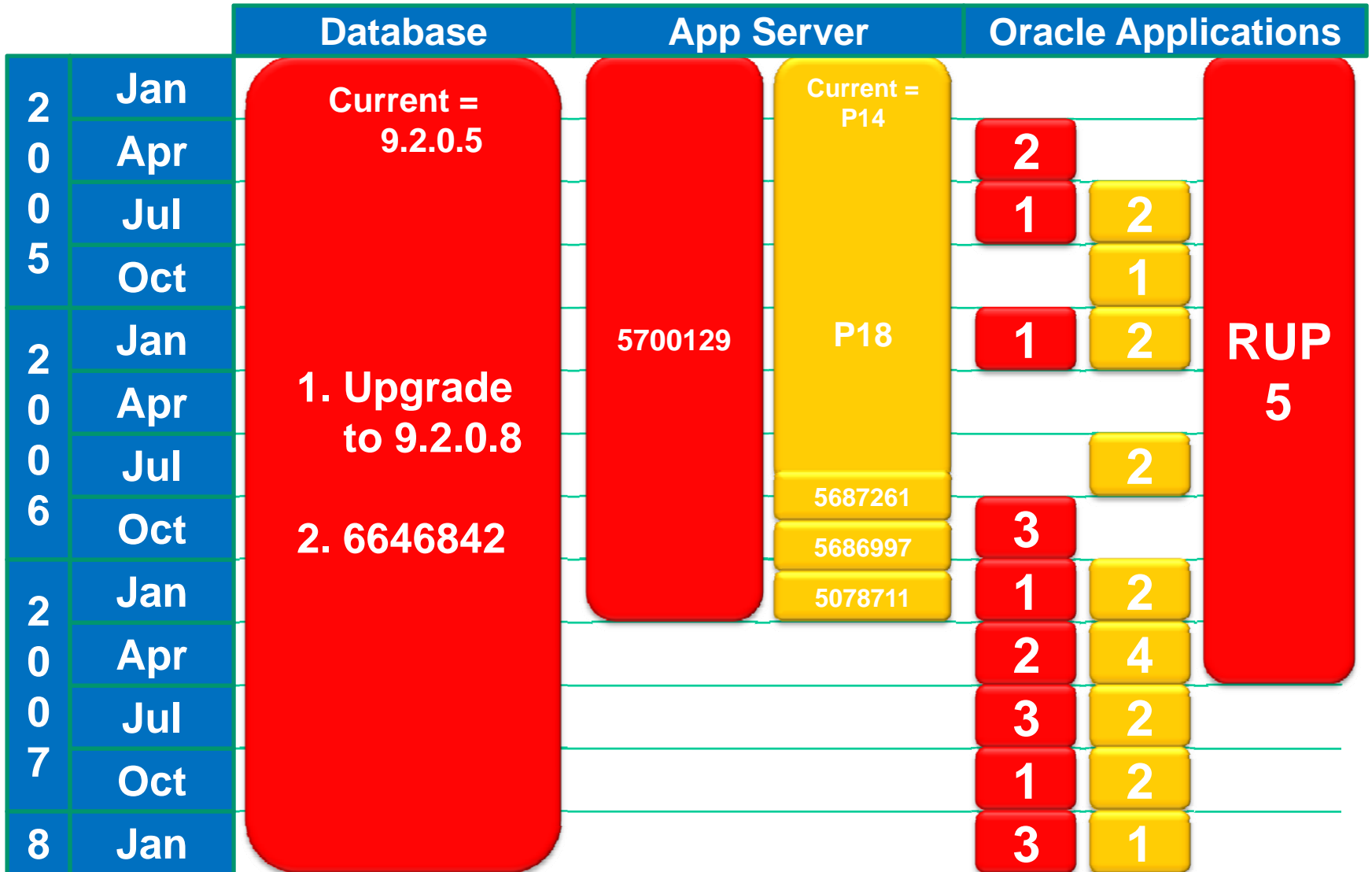
- Oracle Applications 11i
 - July 2008 = no 11.5.9 as Premier Support ends June 2008
- Oracle Database
 - No changes anticipated
- Oracle Application Server
 - No changes anticipated

Database Patches

- Database patches are cumulative for all previous Critical Patch Updates
 - Database patches include non-security fixes
 - Windows patches are really version upgrades
 - Testing should be similar to a version upgrade (i.e., 9.2.0.7 to 9.2.0.8)
 - Some Integrigy clients now only do minimal testing
- Database patches provide the greatest security benefit – Apply them ASAP
 - Apply database patches now, other patches later
 - Otherwise, enable “Managed SQL*Net Access” feature

Oracle Applications Patches (Jan08)

Patches	Scope/ Risk	Patch Complexity	Vulnerability Description and Testing
6640163	Medium	Low	<ul style="list-style-type: none"> ▪ CRM Technology Foundation (JTF) ▪ Cross Site Scripting (XSS) in the jtflogin.jsp page ▪ No testing required ▪ Mandatory for all implementations ▪ External access blocked by URL Firewall
RUP5/6 6530949 RUP4 6701339	High	Low	<ul style="list-style-type: none"> ▪ Oracle Application Library (AOL/FND) ▪ Cross Site Scripting (XSS) in the AppsChangePassword.jsp page ▪ Test basic functionality of the reset password page ▪ Mandatory for all implementations ▪ Not blocked by the URL Firewall and is required



Oracle Applications R12 (Apr08/Unix)

- Oracle Database
 - 10.2.0.3 = 6692464, 6456606, and **6864068** (Cumulative)
- Oracle Application Server
 - 10.1.2.0.2 (Forms) = 6867338 (Cumulative)
 - 10.1.2.2 (Forms) = 6867339 (Cumulative)
 - 10.1.3.0 (OC4J) = 6867341? (Cumulative)
 - 10.1.3.3 (OC4J) = 6867341 (Cumulative)
- Oracle Applications R12
 - Cumulative CPU Patch = 6854598 (5.9 MB)
 - **No Release Update Pack (RUP) this quarter**

Patching Strategy

- General advice –
 - Apply the Database patch – cumulative for all CPUs and previous security alerts
 - Apply Oracle Applications patches – not cumulative, must apply all patches from all previous CPUs
 - Evaluate the effort to apply Developer 6i, Application Server, and JInitiator patches – depending on risk and effort, delaying these patches may be warranted
- Specific advice –
 - Integrity releases guidance for each CPU on our website
 - Each CPU has unique issues and requirements, thus need to be evaluated independently

References

- Integrigy, “Oracle Critical Patch Update April 2008 E-Business Suite Impact”, www.integrigy.com
- Integrigy, “Oracle Jinitiator 1.1.8 Buffer Overflow Vulnerability Analysis”, www.integrigy.com
- Oracle, “Oracle Critical Patch Update April 2008 Advisory”, <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Oracle Corporation, “Oracle E-Business Suite Critical Patch Update Note April 2008”, Metalink Note ID [557157.1](#)
- Oracle Corporation, “Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10”, Metalink Note ID [363827.1](#)
- Oracle Corporation, “Database, FMW, and OCS Software Error Correction Support Policy Version 2.1”, Metalink Note ID [209768.1](#)

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

E-mail: skost@integrigy.com
Phone: 312-961-0215

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681
888/542-4802

Website: www.integrigy.com
Sales: sales@integrigy.com
Development: development@integrigy.com
Support: support@integrigy.com
Security Alerts: alerts@integrigy.com

Copyright © 2008 Integrigy Corporation. All rights reserved.

Questions?